

AMENDMENTS TO THE ABSTRACT:

Please amend the Abstract as follows. Applicants attach to this paper a clean version of the amended Abstract, labeled "Replacement Abstract."

~~A system for method of preventing intrusion in communication traffic with a set of machines in a network includes a data base having stored therein patterns representative of forbidden communication entities as well a firewall module configured for blocking forbidden communication entities in the traffic as identified by respective patterns included in the data base. The system also has another data base having stored therein patterns representative of allowed communication entities for communication with the set of machines and a test system including test facilities replicating the machines in the set. A communication module is configured for allowing communication of allowed communication entities as identified by respective patterns included in the other data base. Unknown communication entities as identified by respective unknown patterns not included in either of the data base and further data base are directed to the test system and run on the test facilities therein to detect possible adverse effects of such unknown communication entities on the test system. The system is further configured so that in the presence of an adverse effect, the unknown communication entity leading to the adverse effect is blocked by the firewall module, and in the absence of an adverse effect, communication of the unknown communication entity failing to lead to the adverse effect is allowed~~ is provided, the traffic including communication entities, including the steps of: providing a test system comprising test facilities replicating at least one of the machines in the set; directing at least part of the communication entities in the traffic toward the test system; running the communication entities directed toward the test system on the test facilities to detect possibly adverse effects on the test system, and i) in the presence of an adverse effect, blocking, by the test system, the communication entities leading to the adverse effect, and ii) in the absence of an adverse effect, allowing, by the test system, the communication entities not having the adverse effect to communicate with the set of machines.